Crafting An Effective Security Organisation

QCon NYC 2015

Rich Smith (@iodboi)

Etsy

$ whoami

- Rich Smith - Brooklyn, NYC
- Director of Security at Etsy
- Co-Founder of Syndis in Reykjavík, Iceland
- Background in breaking not building: Vuln Research, Exploit Dev, Pen-Testing, Attack Framework Dev ...

Etsy Who?

- etsy.com - Craft and vintage marketplace
- Gross Marketplace Sales (GMS) $1.93 Billion in 2014
- 20.8M active buyers, 1.4M active sellers*
- Buying & selling from almost every country in the world
- Offices in 7 countries*, HQ in Brooklyn NYC
- 717 Full Time Employees*, 14 in the tech security team

*As of March 2015

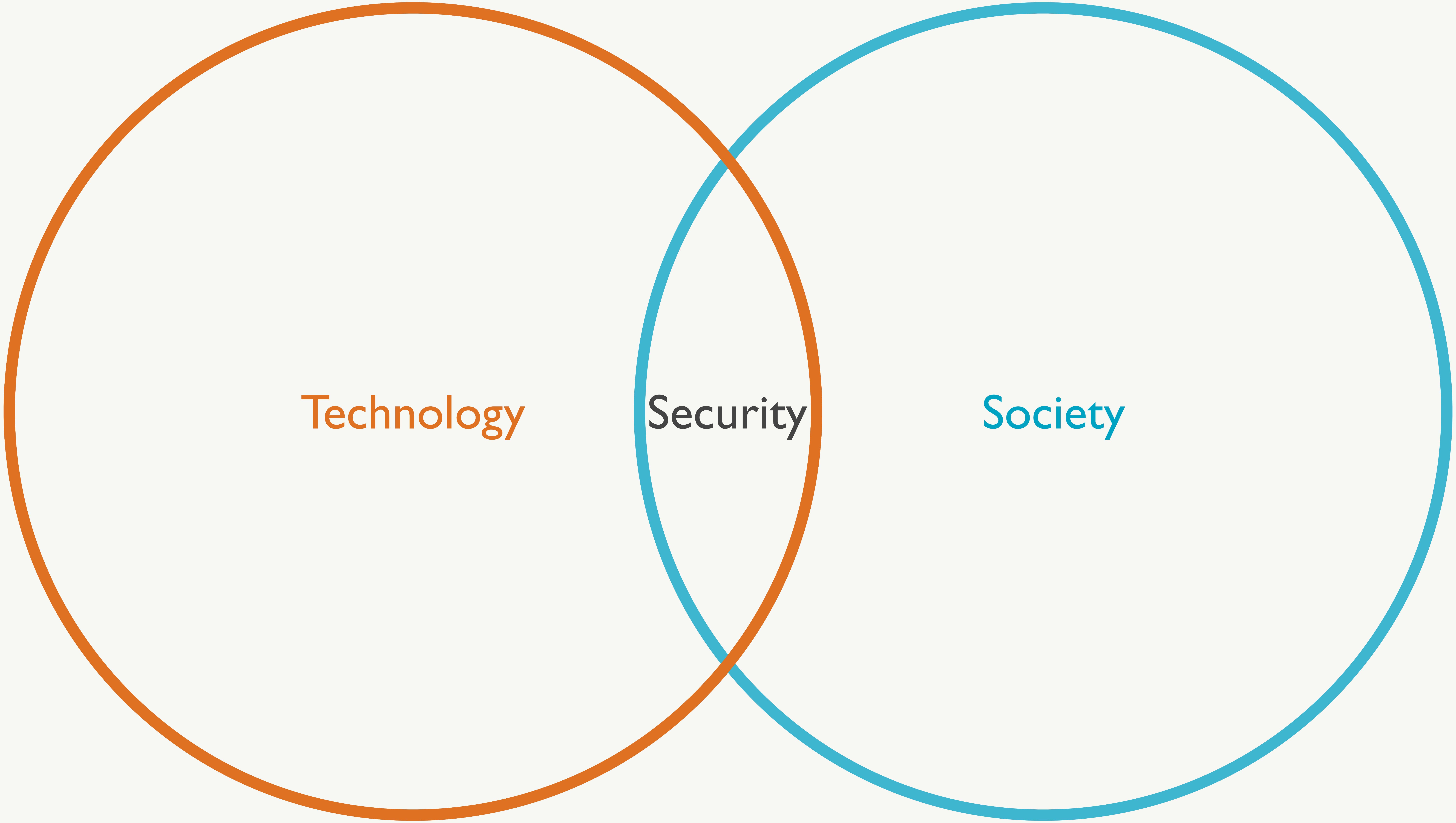
Focus Of Today

- Lessons Learnt & Where We Came From
- Security Mindset & Motivations
- Fostering & Growth of Security Culture

Disclaimer

A + B != Culture

Security from 50,000 ft



Technology

Security

Society

From this perspective it's easy to see that people need to be considered alongside technology for effective security

Security Ego

It doesn't diminish your security cred to value people as much as technology, it just means you will have greater **impact** & **effectiveness**.

You will have more tools to work with.

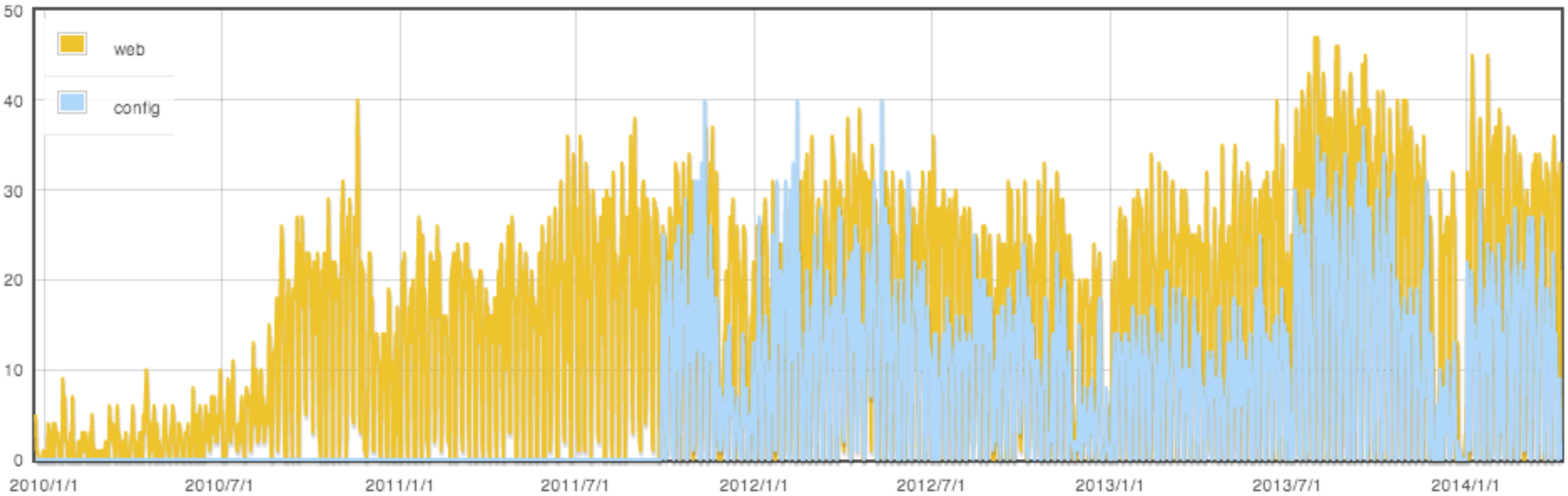
Etsy Engineering Culture

(Some) Core Engineering Principles

- Empower the edges
- Trust but verify
- ‘If it moves graph it’ - Let the data lead you
- ‘Just Ship’ - Get things done
- Every engineer can push to prod at any time

What does Continuous Deployment at Etsy look like?

Pushes Per Day



Very end of 2009

Today

Etsy

@iodboi

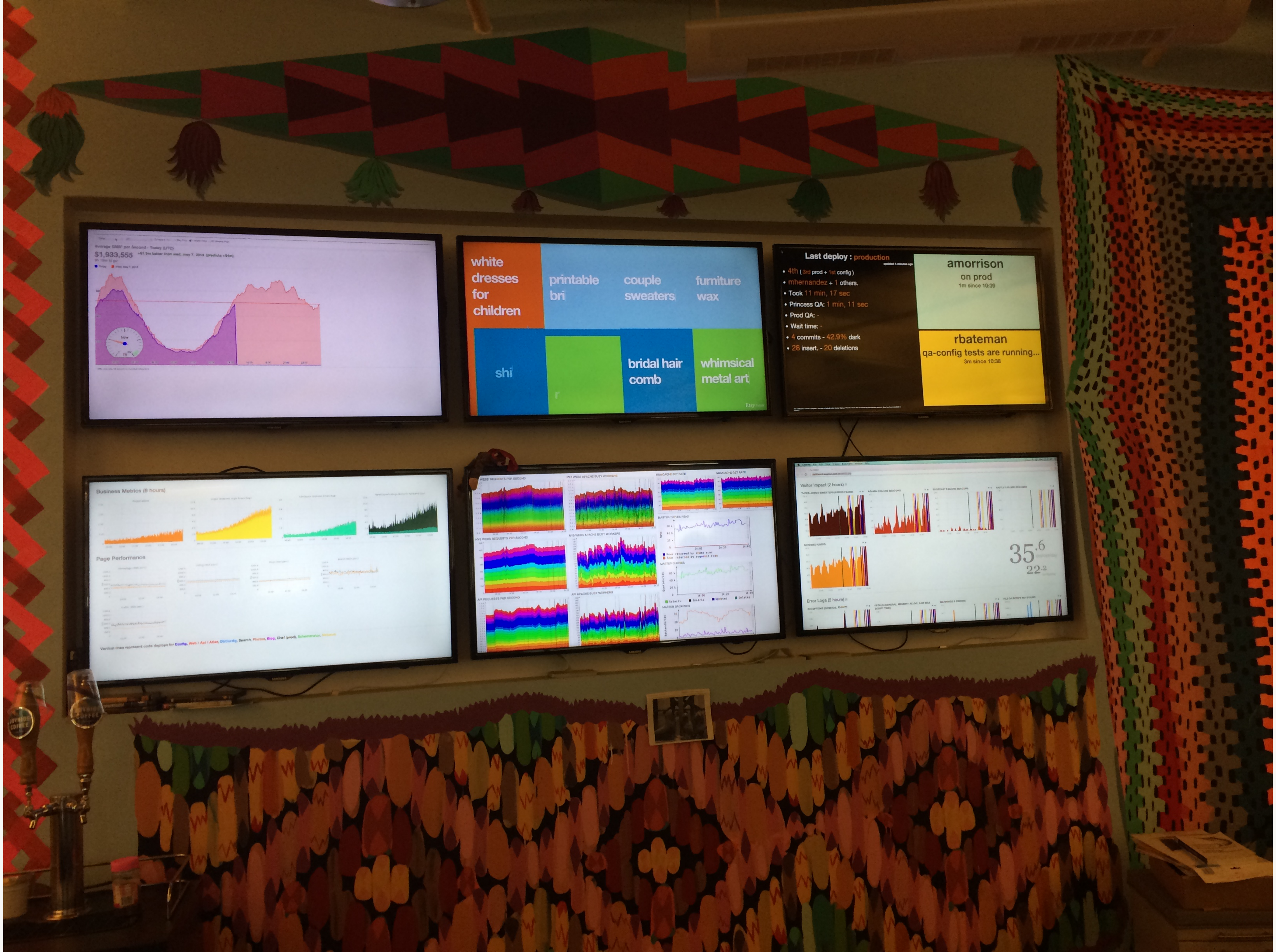
Operator

Config flags

Metrics

http://www.flickr.com/photos/flyforfun/2694158656/

WE HAVE CHARTS & GRAPHS TO BACK US UP
SO FUCK OFF
©2000 DUCK AND COVER OAKLAND, CA STYLE #49
OPSCODE
RULE THE CLOUD
I FAVORITED YOU LAST NIGHT
#monitoring
CODE AS CRAFT
ETSY
C/C
CODEASCRAFT.COM
-STRD-
CAPiTA
www.cfengine.com


$1,933,555
white dresses for children
printable bri
couple sweaters
furniture wax
shi
bridal hair comb
whimsical metal art
Last deploy : production
4th (3rd prod + 1st config)
mhernandez + 1 others.
Took 11 min, 17 sec
Princess QA: 1 min, 11 sec
Prod QA: -
Wait time: -
4 commits - 42.9% dark
28 insert. - 20 deletions
amorrison
on prod
1m since 10:39
rbateman
qa-config tests are running...
3m since 10:36
Business Metrics (8 hours)
Page Performance
Visitor Impact (2 hours)
35.6
22.2
Error Logs (2 hours)

But how do you ‘security’ this anarchy¿

In such an environment classical security approaches don't apply well

Classical == Restrictions

Classical == Blocking

If Security introduces blocking to the org, it will be ignored, not embraced

Continuous Deployment & Security

- The lessons & tools from DevOps are directly applicable
- Apply the same 'if it moves graph it' for security events
- Makes security related data available to everyone
- With CD, no such things as 'out of cycle' patches
- Security engineers push fixes directly to production

‘DevOpsSec’

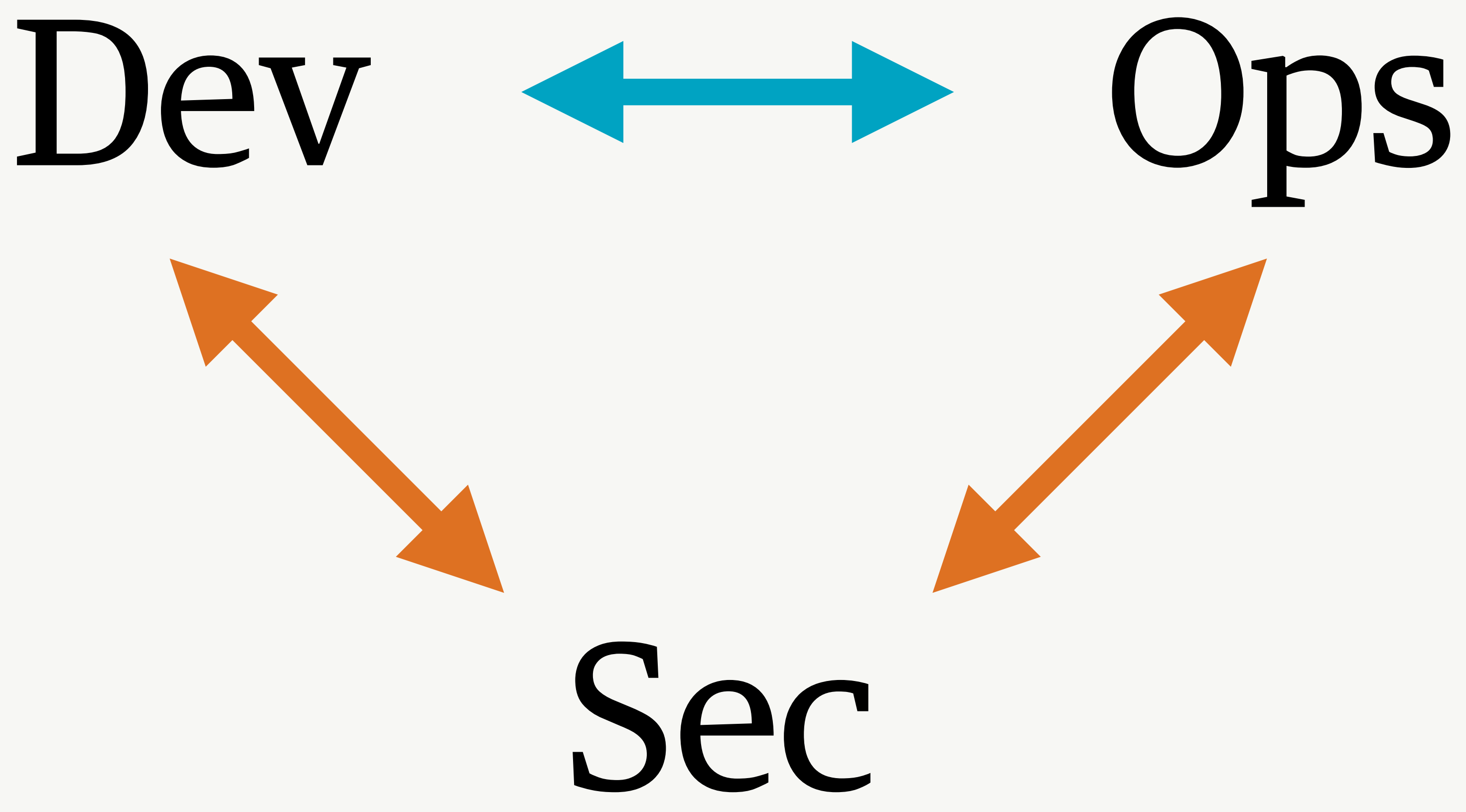
…. or

‘Lessons Security can learn from DevOps’

DevOps

- ‘DevOps’ has become somewhat overloaded
- Aim: Remove silos & organizational blockers between Ops and Developers
- Central to this focus on good Communication & Collaboration

‘DevOpsSec’



- Natural extension of DevOps
- Security faces many of the same challenges as Ops does/did
- Remove barriers between Security, Developers and Ops

The time when a single person or team can be responsible for an orgs security is long over….

….it is up to **EVERYONE**

Security as a Blocker

- Lazy and plain 'bad' security teams default to blocking
- Blocking makes Security a NOP in the CD world
- You will be ignored and teams will work around you
- **No's are a Finite Resource** - use them wisely

Security as a Enabler

- Assisting teams to do their new crazy ideas - securely
- Chase solutions to difficult challenges
  - If your security engineers don't like hard problems and novel solutions you have the wrong ones
- Incentivises proactive engagement with Security

Designated Hackers

- Security engineers assist multiple teams
- ‘Designated’ not ‘Dedicated’
- Breaks down barriers, build trust & relationships
- Represent teams back to security
- Early visibility, input & deeper insight

‘You’re only a blocker if you’re the last to know’

John Allspaw,
Some meeting room, somewhere at Etsy

Principles of Effective Security

3 Principles of Effective Security

1. Enabling
2. Transparent
3. Blameless

Enabling

A security team's success should be measured by what they enable not by what they block

Transparent

A security team that is open as to what it does, and why, spreads understanding and is embraced

Blameless

Security failures will happen, only without blame will you be able to understand the true causes

Progressive Security Culture

Progressive Security Culture

- Understanding that security is as much of a people problem as a technology problem

- As an industry, security has done a poor job of discussing the need for positive security culture

- Often approaches focussed on are entirely technical

- Great culture depends on great people

Security Team Hiring

Number 1 rule ......

Don't Hire Assholes

Security Team Hiring

If you inadvertently do, or you inherit one……

Remove them ASAP

Great culture needs great people

- Abrasive members will be the single biggest factor undermining your progressive security efforts
- Value social skills as highly as technical skills when making your security hires
- 'Cultural fit' critically important

The more diverse a security team, the more approachable it will be to more people

Security Outreach

- Distinct from security education
- Focus on building relationships
    - Removes barriers / reduces intimidation
- Can be as simple as buying cakes or beer!
- Assign budget to this, it will be the best ROI you see

‘Sociable conversation is the **inevitable** product of socializing. Sociable conversation is the way that human beings establish **trusted** relationships among themselves’

Cory Doctorow - Information doesn’t want to be free

Security Candy!

- Biggest source of security pod 'drive bys'
- IRC bot command so people can see what's in stock
- Graph consumption!

Bootcamps

- Have people come and ‘bootcamp’ with security
- Embracing transparency
- Provides insight to daily security issues and concerns
- Build strong personal relationships
- Seed champions back out to the organization

Securgonomics

er·go·nom·ics

ˌərgəˈnämiks/

noun

the study of people's efficiency in their working environment.

secur·go·nom·ics

/səˈkyo͝or/ gəˈnämiks/

noun

the study of the efficiency of people's security interactions in their working environment.

Securgonomics

- Lowering the barrier to interact with security
- Too often security teams lock themselves away
- Being accessible & visible to everyone is invaluable
- Sit on the busiest office pathway you can
- Have your security dashboards front & centre

Blameless Postmortems

- Comes from our desire to have Just Culture
- Aim to learn from failings not to target blame
- Share detailed accounts of actions, decisions and circumstances without fear of punishment or retribution
- Empower engineers to own their own stories
- Applies to Security failures as much as Ops failures

Blameless Postmortems

‘We must strive to understand that accidents don’t happen because people gamble and loose. Accidents happen because the person believes that what is about to happen:

- Is not possible
- Has no connection to what they are doing
- The intended outcome is worth the risk’

Erik Hollnagel

Blameless postmortem blog post by John Allspaw:

codeascraft.com/2012/05/22/blameless-postmortems

Indicators of an Effective Security Team

Is Data Driven

- Too often security is explained with religious conviction
- Security is not black and white, many shades of grey
- Security is not a point but a vector
- Gather data to support security decisions and let it lead you to the correct shade of grey

Runs a Bug Bounty

- Continuous Assessment of your security program
  - D'ya you think you're not under attack 24/7 anyway ....
- Raises cost of attack for real adversaries
- Increases value from focused pentests/red teaming
- Generates good metric sets about security (data driven)

Doesn't Cry Wolf

- Verify issues before raising them to developers
- They will only chase their tail a few times before ignoring
- Security engineers should be in amongst the codebase
    - Aim to own the entire fix process themselves

Makes Realistic Tradeoffs

- Not everything is critical
- Understand impact
- Let low risk issues ship & getting commitments to a reasonable remediation window buys you lots
- **No's are a Finite Resource** - use them wisely

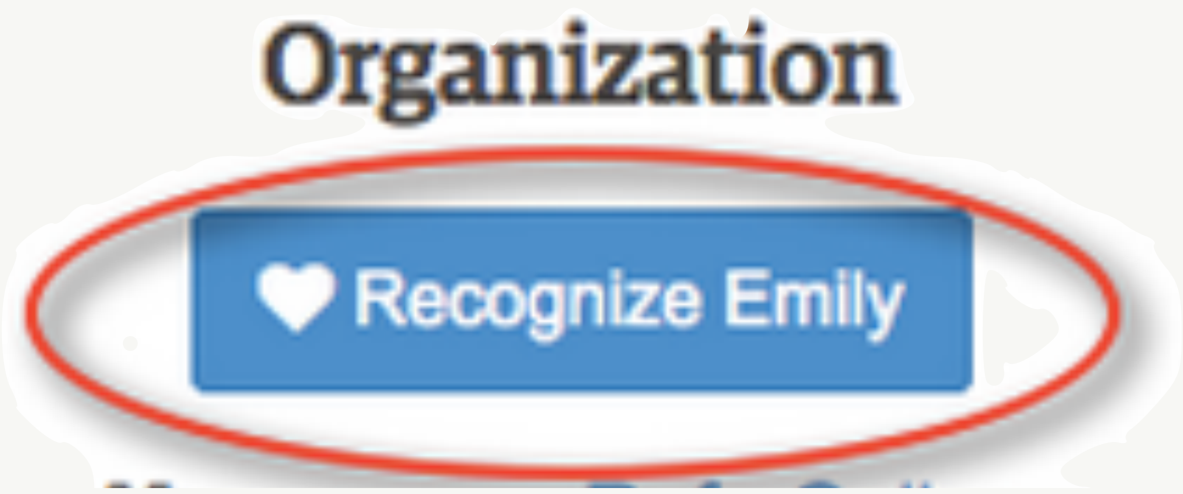
Provides Context & Impact

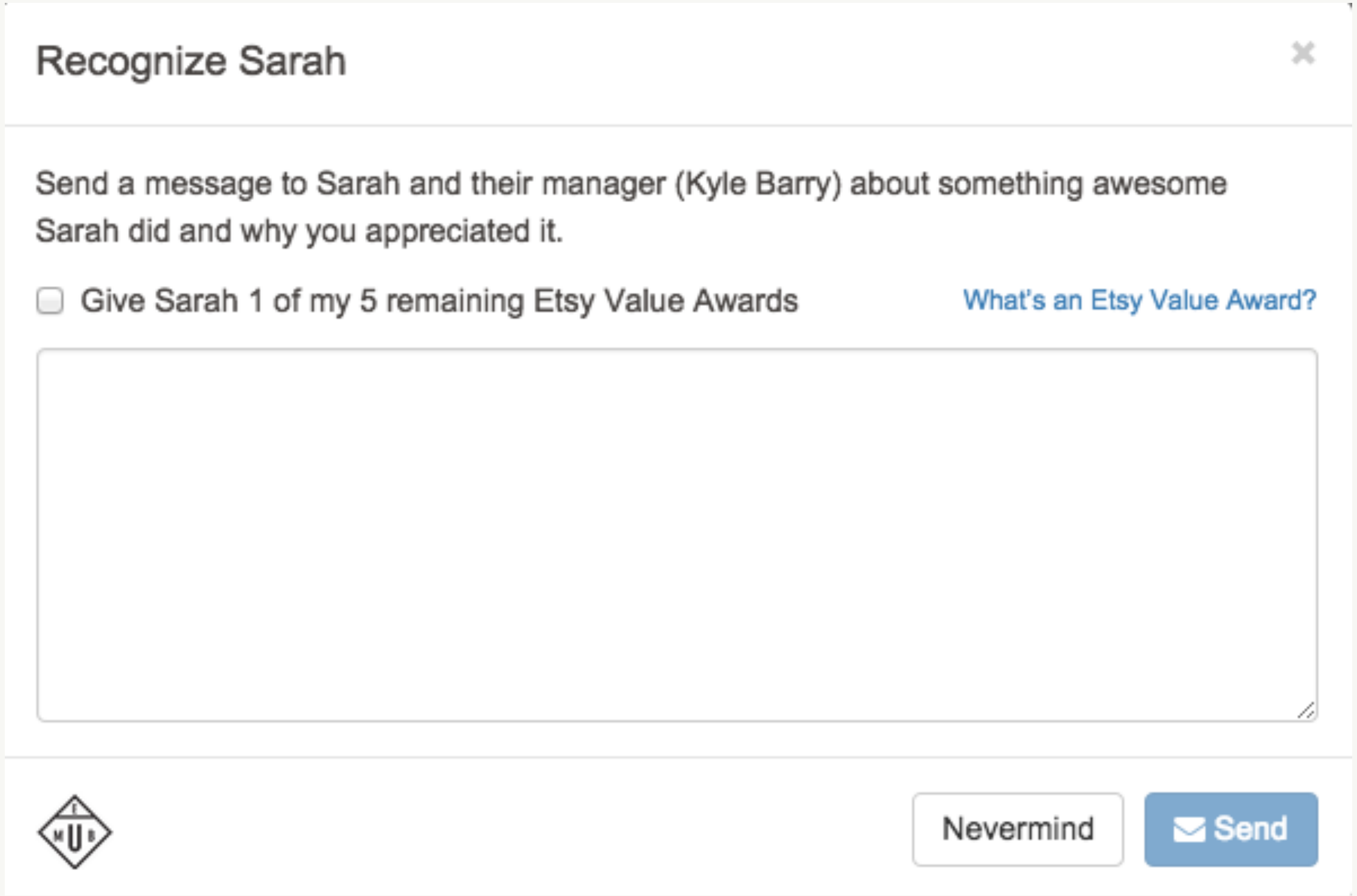
- Explaining why something is an issue and what it may result in to the team affected
- Provides security education and garners understanding
- 'This would allow an attacker to impersonate another user & read their mail' is useful, starts dialogues ....
- 'Input validation was insufficiently applied' doesn't

Recognises & Rewards

- Rewarding folks in the org who reach out to Security
- We do this is a number of ways:
  - Pins and patches
  - T-Shirts
  - Etsy gift vouchers
  - IRC Pluses & Value Awards
  - Thanking people for raising issues

Etsy Value Awards





Recognize Sarah

Send a message to Sarah and their manager (Kyle Barry) about something awesome Sarah did and why you appreciated it.

□ Give Sarah 1 of my 5 remaining Etsy Value Awards

Treats Security as a BRAND

- Your security culture has real value

- Work long & hard to build it up

- Can however be damaged in the blink of an eye

- Aim to build strong, positive, long term associations with the security team org wide

- Get your peers to buy into security

Wrap up

Final thoughts

- Building an effective security organisation takes effort
- Requires a focus on people as much as technology
- Learn from DevOps & move to a DevOpsSec mindset
- Enable don't block, else you'll make security a NOP

Enabling. Transparent. Blameless

We’re Hiring!
etsy.com/careers

(Conditions apply, see slide 40….!)

<link />

Blog	sin-ack.co.uk
Presentations	speakerdeck.com/iodboi
Tweetz	twitter.com/iodboi
Code	github.com/mynameismeerkat